Koneru Lakshmaiah Education Foundation
(Deemed to be University estd. u/s. 3 of the UGC Act, 1956)
Off-Campus: Bachupally-Gandimaisamma Road, Bowrampet, Hyderabad, Telangana - 500 043.
Phone No: 7815926816, www.klh.edu.in

Case Study ID: 1

Enhancing Wireless Network Security at a University

2. Introduction

- **Overview**: This case study explores the wireless network security challenges faced by a university and a large corporation, both of which experienced unauthorized access and data breaches. The study highlights the strategies and technologies implemented to enhance network security, including segmentation, upgraded protocols, and employee training.
- **Objective**: The objective is to demonstrate how effective security measures, such as network segmentation, the adoption of WPA3, and strong authentication protocols, can mitigate risks and protect sensitive data within wireless networks.

3. Background

- **Organization/System Description**:
  - *University*: A large campus with multiple buildings and thousands of students, staff, and guests accessing the wireless network daily.
  - *Corporation*: A global enterprise with a vast wireless network used by employees, clients, and partners.
- **Current Network Setup**:
  - *University*: A single, unified wireless network serving all users, with outdated security protocols.
  - *Corporation*: A wireless network relying on WPA2 for security, which is vulnerable to attacks like KRACK.

4. Problem Statement

- **Challenges Faced**:
  - *University*: Frequent unauthorized access leading to data breaches and service disruptions, causing reputational damage.
  - *Corporation*: A security breach due to the KRACK vulnerability in WPA2, exposing sensitive information to potential attackers.

5. Proposed Solutions

- **Approach**:
  - *University*: Implement network segmentation based on user roles, upgrade to WPA3 Enterprise, and introduce strong authentication methods.

  - *Corporation*: Transition to WPA3, employ 802.1X authentication, and enhance network segmentation to protect critical systems.
- **Technologies/Protocols Used**:
  - WPA3, 802.1X, AES-256 encryption, Intrusion Detection and Prevention Systems (IDPS), Role-Based Access Control (RBAC).

6. Implementation

- **Process**:
  - *University*: Segmentation of the network, deployment of WPA3 and 802.1X, and installation of IDPS. Security awareness training for staff.
  - *Corporation*: Upgrade from WPA2 to WPA3, implementation of 802.1X, and network segmentation.
- **Implementation Timeline**:
  - *University*: Over a six-month period, including planning, testing, and deployment phases.
  - *Corporation*: A three-month period for the transition to WPA3 and security updates.

7. Results and Analysis

- **Outcomes**:
  - *University*: Significant reduction in unauthorized access, improved data security, enhanced network reliability, and a strengthened reputation.
  - *Corporation*: Successful mitigation of risks associated with WPA2, prevention of further breaches, and increased network security.
- **Analysis**:
  - The implementation of advanced security protocols and network segmentation was crucial in addressing the vulnerabilities. Both organizations saw marked improvements in their network security posture.

8. Security Integration

- **Security Measures**:
  - Continuous monitoring via IDPS, regular security audits, vulnerability assessments, and employee training were integral to maintaining a secure network environment.

9. Conclusion

- **Summary**: By adopting proactive security measures, both the university and the corporation were able to safeguard their wireless networks against unauthorized access and data breaches. The case study illustrates the importance of staying updated with the latest security protocols and regularly assessing network vulnerabilities.

- **Recommendations**: Organizations should regularly upgrade their security protocols, implement network segmentation, and conduct frequent security training and audits to ensure the continued protection of their networks.

10. References

- *Citations*: Reference research papers and articles related to wireless network security, WPA3, network segmentation, and the KRACK vulnerability for further reading and validation of the case study.
- Reference: https://www.researchgate.net/profile/Imam-Riadi-2/publication/348717236_Optimation_Wireless_Security_IEEE_8021X_using_the_Extensible_Authentication_Protocol-Protected_Extensible_Authentication_Protocol_EAP-PEAP/links/600c9a07a6fdccdcb87725e9/Optimation-Wireless-Security-IEEE-8021X-using-the-Extensible-Authentication-Protocol-Protected-Extensible-Authentication-Protocol-EAP-PEAP.pdf
- https://ieeexplore.ieee.org/abstract/document/1286832?casa_token=WvOf9pvkmc4AAAAA:W4KSI8KBw5YLbJqyYWKrFjaaXCLS0kKqoor9TNCzi6QIh2drB38V4ntRhTUajpF1xg5jycaELFgH
- https://openurl.ebsco.com/EPDB%3Agcd%3A15%3A4339519/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A91876331&crl=c

NAME: Mahalakshmi Munichitti Satish

ID-NUMBER: 2320030218

SECTION-NO: 4